Analyzing WannaCry Ransomware Considering the Weapons and Exploits

Da-Yu KAO*, Shou-Ching HSIAO**, Raylin TSO***

*Department of Information Management, Central Police University, Taoyuan City 333, Taiwan

**Haishan Precinct, New Taipei City Police Department, New Taipei City 220, Taiwan

***Department of Computer Science, National Chengchi University, Taipei 116, Taiwan

dayukao@gmail.com, oliver84312@gmail.com, raylin@cs.nccu.edu.tw

***Abstract*—As ransomware has increased in popularity, its creators are using our fears to their advantage. The rapid proliferation of ransomware attacks indicates the growing tendency of ransomware-as-a-service (RaaS) and the integration of hacking weapons. This paper presents the analysis of the infamous WannaCry ransomware, which is one of the most propagated and damaging malware in 2017. The anatomy of ransomware attacks is discussed to understand the multi-phased execution of WannaCry, including the deployment, installation, destruction, and command-and-control. The chain of WannaCry's execution comprises several hacking weapon components. WannaCry not only embeds the binary in the resource section for multi-phased execution, but also implements a strong encrypting algorithm and a key structure. A reverse engineering analysis of each component, along with the network analysis of WannaCry's exploits offers an insight into the inner design of WannaCry. The observations of this research contribute to recent security systems and future defense strategies.**

***Keyword*—Ransomware, Reverse Engineering Analysis, Network Analysis, Hacking Weapons, WannaCry Exploits**

Da-Yu Kao received the B.S. and M.S. degree in information management from Central Police University, Taiwan, in 1993 and 2001, the Ph.D degrees in Crime Prevention and Correction from Central Police University, Taiwan, in 2009, respectively. From 1993 to 1996, he was with Taipei City Police Department, Taiwan, where he was an information technology police officer involved in the development of policing information systems. From 1996 to 2007, he was with Criminal Investigation Bureau, National Police Administration, Taiwan, where he was a detective and forensic police officer in cybercrime investigation and digital forensics. From 2007 to 2013, he was with Maritime Patrol Directorate General, Coast Guard Administration, Taiwan, where he was an information technology section chief in the department of information and communication. Since 2013, he has been with Central Police University, Taiwan, where he is currently an associate professor in the Department of Information Management. His research interests include cybercrime investigation, digital forensics, digital evidence, information management, criminal profiling, and cyber criminology.

Shou-Ching Hsiao received the B.S. degree in information management from Central Police University, Taiwan, in 2016. Since 2016, she has been with Haishan Precinct, New Taipei City Police Department, Taiwan, where she is currently an information lieutenant and is responsible for information system management, information security, malware analysis, and real-time video for security control. In 2018, she is also working toward the M.S. degree in the Department of Computer Science, National Chengchi University, Taiwan. Her current research interests include malware analysis, cybercrime investigation, digital forensics, digital evidence, information management, criminal profiling, and cyber criminology.

Raylin Tso received the B.S. degree in Industrial Engineering from National Tsing Hua University, Hsinchu, Taiwan and M.S. degree in Management Science - Division of Management and Public Policy, University of Tsukuba, Tsukuba, Ibaraki, Japan, in 2002, M.S. degree in Risk Engineering, Graduate School of Systems and Information Engineering, University of Tsukuba, Tsukuba, Ibaraki, Japan, in 2004, the Ph.D degrees in Risk Engineering, Graduate School of Systems, University of Tsukuba, Tsukuba, Ibaraki, Japan, in 2006, respectively. From 2006 to 2008, he was with Graduate School of Systems and Information Engineering, University of Tsukuba, Japan, where he was an academic researcher. Since 2008, he has been with National Chengchi University, Taiwan, where he is currently an associate professor and chairman in the Department of Computer Science. His research interests include cryptography, information security, post-quantum, blockchain and privacy enhancement.